IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

IN RE DEALER MANAGEMENT SYSTEMS ANTITRUST LITIGATION, MDL 2817	)	Case No. 18-cv-864
	)	Judge Robert M. Dow, Jr.
This document relates to:	)	
THE DEALERSHIP CLASS ACTION	)	

MEMORANDUM OPINION AND ORDER

Before the Court is the motion to dismiss the counterclaims of Defendant/Counter-Plaintiff CDK Global, LLC ("Counter-Plaintiff" or "CDK") [593] filed by Plaintiffs/Counter-Defendants ACA Motors, Inc.; Continental Classic Motors, Inc.; 5800 Countryside, LLC; HDA Motors, Inc.; H & H Continental Motors, Inc.; Continental Autos, Inc.; Naperville Zoom Cars, Inc.; NV Autos, Inc.; Baystate Ford Inc.; Cliff Harris Ford, LLC; Marshall Chrysler Jeep Dodge, L.L.C.; Warrensburg Chrysler Dodge Jeep, L.L.C.; Cherry Hill Jaguar; JCF Autos LLC; Jericho Turnpike Sales LLC; Patchogue 112 Motors LLC; and Waconia Dodge, Inc. (collectively, "Counter-Defendants"). For the reasons set forth below, the motion to dismiss [593] CDK's counterclaims is granted in part and denied in part. CDK is given until September 30, 2019 to file amended counterclaims consistent with this opinion.

I. Background[1]

Given that this case already has been extensively litigated before multiple courts, the Court assumes some familiarity with the background of this case and thus will limit its recitation of the

[1] For purposes of the motions to dismiss, the Court accepts as true all of Counter-Plaintiff's well-pleaded factual allegations and draws all reasonable inferences in Counter-Plaintiff's favor. *Killingsworth v. HSBC Bank Nev., N.A.*, 507 F.3d 614, 618 (7th Cir. 2007).

facts essential to the motion now before it. CDK brings counterclaims against the Counter-Defendants under the Computer Fraud and Abuse Act, the Digital Millennium Copyright Act, and for breach of contract. The counterclaims focus on Counter-Defendants' purported unauthorized access—along with data integrator Authenticom, Inc.—of CDK's enterprise software and computing platform for automotive dealerships and dealership groups known as its Dealer Management System or, more commonly, its DMS.

The automotive data system that CDK supports is massive—with tens of thousands of installations of approved vendor applications and millions of transactions every day—supporting hundreds of billions of dollars in commerce each year. [522 (Counterclaims), at ¶ 5.] CDK has made tremendous investments to build out and support its network of product and service offerings. [*Id*.] Over the last four years alone, CDK has spent more than $480 million researching, developing, and deploying new and enhanced product solutions for its customers. [*Id*.] CDK's DMS includes (and is largely comprised of) valuable pieces of intellectual property, including patented technologies, proprietary software elements and programs that it has created (including software programs protected by the copyright laws), and proprietary data collections, which are accessible through the DMS. [*Id*. at ¶ 32.] Dealers that purchase DMS services from CDK are granted a personal, non-transferable license to use CDK's DMS in accordance with the terms and conditions of their agreements. [*Id*.]

CDK's DMS offering consists of software and hardware components residing at both the dealership and at CDK's data centers ("CDK's network"). [*Id*. at ¶ 33.] CDK uses state-of-the-art technology to secure the connections between the dealerships and CDK's network, including through specialized hardware at each dealership site. [*Id*.] That hardware creates a "virtual private network" or "Leased-Line Multiprotocol Label Switching network" between the dealership and

CDK's network, which accepts direct communications only from computers on the corresponding dealership's network. [*Id*.]

CDK's DMS is password protected. [*Id*. at ¶ 37.] To access the DMS, each dealership employee must use his or her individual login credentials. [*Id*.] CDK has implemented security features in addition to password protection. [*Id*. at ¶ 40.] In early 2016, CDK created a login prompt requiring users to certify that they were an "authorized dealer employee" before they could access CDK's DMS. [*Id*.] Further, in November 2017, CDK began introducing a CAPTCHA[2] control for particular login credentials that it suspected were being used to facilitate unauthorized access to its DMS by third parties. [*Id*. at ¶ 41.] Humans can easily pass CAPTCHA tests, but automated scripts—like those used by Authenticom and other third-party data extractors—often encounter difficulty. [*Id*.] The CAPTCHA controls are specifically designed to prevent access to computers through automated means. [*Id*.]

CDK has entered into a Master Service Agreement ("MSA") with each Counter-Defendant (collectively, the "MSAs"). [*Id*. at ¶ 43.] The MSAs expressly prohibit Counter-Defendants from supplying DMS login credentials to third parties or otherwise granting third parties access to CDK's DMS. [*Id*.] Specifically, Section 6(D) of the MSAs provides that the "Client shall not allow access to [CDK's DMS] by any third parties except as otherwise permitted by this agreement." [*Id*. at ¶ 44.] In addition, each Counter-Defendant expressly agrees that it will only use CDK's software "for its own internal business purposes and will not sell or otherwise provide, directly or indirectly, any of the Services or Software, or any portion thereof, to any third party" and that it will "treat as confidential and will not disclose or otherwise make available any of the

[2] "CAPTCHA" is an acronym for "Completely Automated Public Turing Test to tell Computers and Humans Apart." *Tel. Sci. Corp. v. Asset Recovery Sols., LLC*, 2016 WL 4179150, at *1 (N.D. Ill. Aug. 8, 2016).

[CDK's] Products (including, without limitation, screen displays or user documentation) or any * * * proprietary data, information, or documentation related thereto * * * in any form, to any person other than employees and agents of [the dealer.]" [*Id*. at ¶ 45.] Each dealer acknowledges that—notwithstanding its license to use CDK's DMS—the DMS remains at all times "the exclusive and confidential property of [CDK]." [*Id*.] Additionally, the MSAs independently prohibit "ANY THIRD PARTY SOFTWARE TO ACCESS [CDK'S] DEALER MANAGEMENT SYSTEM EXCEPT AS OTHERWISE PERMITTED BY THIS AGREEMENT." [*Id*. at ¶ 46.]

CDK contends that third party hostile data extractors like Authenticom are not "agents" of the Counter-Defendants. [*Id*. at ¶ 49.] Authenticom's own contract with dealers makes clear that Authenticom is not the dealer's "agent," and in fact refers to "agents" of the dealer repeatedly as third parties to the agreement. [*Id*.] Similarly, the standard End-User License Agreement ("EULA") offered by Superior Integrated Solutions ("SIS"), another third party data extractor, states that "[t]he parties shall be independent contractors under this Agreement, and nothing herein will constitute either party as the employer, employee, agent or representative of the other party, or both parties as joint ventures or partners for any purpose." [*Id*.]

CDK submits that Counter-Defendants have repeatedly breached their contracts with CDK by handing out their DMS login credentials (directly or through their software vendors) to third party data extractors for the express purpose of enabling those third parties to use those credentials to repeatedly and relentlessly access CDK's DMS using sophisticated computer software that extracts (or scrapes) large volumes of data from the system. [*Id*. at ¶ 2.] Many of these data extractors—including Authenticom—then resell that data to other third-party application providers, paying nothing to CDK. [*Id*.] According to CDK, this unauthorized access not only

threatens the security of the data in CDK's DMS, but also threatens the integrity of that data because ungoverned extraction and insertion of data into the DMS may corrupt the DMS databases. [*Id*.] Moreover, the thousands of unauthorized extractions and the high volume of data in many of those extractions degrade the performance of the DMS, impairing its value for all of CDK's DMS customers. [*Id*.]

CDK brings counterclaims against Counter-Defendants based on this alleged unauthorized access. Before the Court is Counter-Defendants' motion to dismiss the breach of contract, Computer Fraud and Abase Act, and Digital Millennium Copyright Act counterclaims brought against them.

II. Legal Standard

To survive a Federal Rule of Civil Procedure ("Rule") 12(b)(6) motion to dismiss for failure to state a claim upon which relief can be granted, the complaint first must comply with Rule 8(a) by providing "a short and plain statement of the claim showing that the pleader is entitled to relief," Fed. R. Civ. P. 8(a)(2), such that the defendant is given "fair notice of what the * * * claim is and the grounds upon which it rests." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007) (quoting *Conley v. Gibson*, 355 U.S. 41, 47 (1957)) (alteration in original). Second, the factual allegations in the complaint must be sufficient to raise the possibility of relief above the "speculative level." *E.E.O.C. v. Concentra Health Servs., Inc.*, 496 F.3d 773, 776 (7th Cir. 2007) (quoting *Twombly*, 550 U.S. at 555). "A pleading that offers 'labels and conclusions' or a 'formulaic recitation of the elements of a cause of action will not do.'" *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Twombly*, 550 U.S. at 555). Dismissal for failure to state a claim under Rule 12(b)(6) is proper "when the allegations in a complaint, however true, could not raise a claim of entitlement to relief." *Twombly,* 550 U.S. at 558. In reviewing a motion to dismiss pursuant to

Rule 12(b)(6), the Court accepts as true all of Counter-Plaintiff's well-pleaded factual allegations and draws all reasonable inferences in Counter-Plaintiff's favor. *Killingsworth v. HSBC Bank Nev., N.A.*, 507 F.3d 614, 618 (7th Cir. 2007).

III. Analysis

A. Breach of Contract (First Counterclaim)

CDK's first cause of action alleges that the Counter-Defendants violated the terms of their respective MSAs by sharing login credentials with Authenticom and other third parties. CDK further contends that Counter-Defendants have "repeatedly violated the express contractual prohibitions" in their respective MSAs by "actively facilitating hostile, unauthorized access to CDK's DMS." [522 (Counterclaims), at ¶ 103, 104-32.] The MSAs "expressly prohibit the Counter-Defendants from allowing third-parties to access CDK's DMS." [*Id*. at ¶ 43.] There is a limited exception to this prohibition in some MSAs that allows access by "employees and agents of [the dealer] with a need-to-know." [*Id*. at ¶ 49.] Counter-Defendants argue that CDK's breach of contract counterclaim fails because Counter-Defendants authorized data extractors to extract data from the DMS, which—according to Counter-Defendants—is all that is necessary under the MSAs. Specifically, CDK alleges:

> In knowingly providing login credentials to these data extractors and, actively or passively, "authorizing" them to access CDK's DMS to extract or insert data—including data that does not belong to the Dealership Counter-Defendants—the Dealership Counter-Defendants have breached their contracts with CDK. This conduct also violates the CFAA, which prohibits unauthorized access to protected computer systems. In addition, certain Dealership Counter-Defendants—and numerous members of the putative class—have engaged in further unlawful conduct that violates the DMCA. CDK requests that the Court enjoin the Dealership Counter-Defendants' illegal conduct and award CDK damages.

[*Id*. at ¶ 3.] According to Counter-Defendants, this allegation establishes that Authenticom and other third-party integrators were authorized to access CDK's data and therefore were acting as

the agents of Counter-Defendants. CDK responds that the word "authorizing" is in quotation marks because CDK is alleging that third-party access to its data *was not* authorized. *Stone v. Wright*, 734 F. App'x 989 (7th Cir. 2018) (using scare quotes around claim brought by plaintiff to express doubts regarding viability of such a claim under the Constitution). The Court agrees that the use of the term "authorizing" in scare quotes does not amount to a concession that Counter-Defendants' access to CDK's data was authorized.

That leaves the question of whether Authenticom and other third-party data integrators were the employees and/or agents of Counter-Defendants such that they were authorized to access CDK's DMSs under the terms of the relevant MSAs. Because Counter-Defendants do not contend that Authenticom and other third-party data integrators were their employees, the Court need only consider whether the third-party data integrators were the agents of Counter-Defendants. To the extent that Counter-Defendants contend that all that is needed to circumvent the MSAs' prohibition on allowing parties to access CDK's DMS was Counter-Defendants' authorization, the prohibition on third-party access would be pointless, as Counter-Defendants simply could authorize any third-party to access CDK's DMS. Thus, something more than authorization by Counter-Defendants' must be necessary to establish agency under the MSAs. *Cress v. Recreation Servs., Inc.*, 795 N.E.2d 817, 852 (Ill. App. Ct. 2003) ("[A] court must give meaning and effect to every part of the contract.").

Counter-Defendants argue that—to the extent that the term "agents" is ambiguous—the term should be construed against CDK, as the drafter of the MSAs. *Bourke v. Dun & Bradstreet Corp.*, 159 F.3d 1032, 1036 (7th Cir. 1998) (Under Illinois law, "any ambiguity in the terms of a contract must be resolved against the drafter of the disputed provision." (quoting *Dowd & Dowd, Ltd. v. Gleason*, 693 N.E.2d 358, 368 (Ill. App. Ct. 1998) (internal quotation marks omitted)). But

agency is a concept well-defined and understood under the law and by businesses of even modest sophistication—a threshold that all of the parties to this motion easily clear. *Hernandez ex rel. Gonzalez v. Tapia*, 2010 WL 5232942, at *7 (N.D. Ill. Dec. 15, 2010) ("The phrase 'agents and employees' is not ambiguous and therefore the court will apply the plain meaning of these terms.").

Moreover, agency is an issue of fact generally not susceptible to resolution at the motion to dismiss stage. *Restoration Specialists, LLC v. Hartford Fire Ins. Co.*, 2009 WL 3147481, at *3 (N.D. Ill. Sept. 29, 2009) ("[T]he question of agency typically presents an issue of fact that seldom can be resolved at the summary judgment stage, much less on a motion to dismiss."); *Semitekol v. Monaco Coach Corp.*, 582 F. Supp. 2d 1009, 1024 (N.D. Ill. 2008) ("[W]hether an agency relationship has been established between the parties is [an issue] of fact which is not properly resolved on a motion to dismiss." (citation omitted)). Under Illinois law—on which Counter-Defendants rely in their reply brief—"[t]he analysis turns primarily on the level of control that the alleged agent retains over the performance of its assigned work". *Jackson v. Bank of New York*, 62 F. Supp. 3d 802, 814 (N.D. Ill. 2014) (citing *Horwitz v. Holabird & Root*, 816 N.E.2d 272, 279 (2004)). "In a principal-agent relationship, the principal retains the right to control the manner and method in which the work is carried out by the agent." *Id*. (citing *Uesco Indus., Inc. v. Poolman of Wis., Inc.*, 993 N.E.2d 97, 112 (Ill. App. Ct. 2013)). "By contrast, '[a]n independent contractor is one who undertakes to produce a given result but in the actual execution of the work is not under the orders or control of the person for whom he does the work but may use his own discretion in things not specified * * * [and] without his being subject to the orders [of the person for whom the work is done] in respect to the details of the work." *Id*. (quoting *Horwitz*, 816 N.E.2d at 279). Other factors that bear on the question of whether one is properly considered an agent or an independent contractor include "(1) the question of hiring; (2) the right to discharge; (3) the manner

of direction of the servant; (4) the right to terminate the relationship; and (5) the character of the supervision of the work done." *Lawlor v. N. Am. Corp. of Ill.*, 983 N.E.2d 414, 427 (Ill. 2012). Counter-Defendants fail to explain how this analysis can be resolved as a matter of law based on the allegations in the breach of contract counterclaim.

In fact, CDK identifies allegations suggesting that there is no such agency relationship. CDK alleges that Authenticom's own contract with dealers makes clear that Authenticom is not the dealer's "agent," and in fact refers to "agents" of the dealer repeatedly as third parties to the agreement. [522 (Counterclaims), at ¶ 49.] Similarly, SIS's EULA states that "[t]he parties shall be independent contractors under this Agreement, and nothing herein will constitute either party as the employer, employee, agent or representative of the other party, or both parties as joint ventures or partners for any purpose." [*Id*.]

Counter-Defendants counter that the contracts do not undermine their contention that data integrators are their agents. Specifically, Counter-Defendants note that an agent may be both an independent contractor in one relationship and an agent in another. *Signs & Blanks, Ltd. v. Lanan Prod., Inc.*, 2009 WL 10695777, at *5 n.4 (N.D. Ill. Jan. 20, 2009) ("[A] person may be both an independent contractor and an agent with the authority both to control the details of the work and also the power to act for and to bind the principal in business negotiations within the scope of [the] agency." (internal quotation marks and citation omitted)). Although Counter-Defendants do not identify what law applies to this analysis in their opening brief, Counter-Defendants assert in their reply brief that Illinois law applies to the issue of whether data extractors were agents of Counter-Defendants.[3] Illinois courts have indicated that an independent contractor may be

[3] The Court questions whether Illinois law applies, as the contract between dealers and Authenticom is governed by Wisconsin law. [See 506.] Because the parties have not presented any argument to that effect, the Court proceeds on the assumption that Illinois law applies. In any event, the result likely would be the same under Wisconsin law. As the Court previously has noted, the distinction under Wisconsin law

considered an agent for certain purposes when they have "the authority both to control the details of the work and also 'the power to act for and to bind the principal in business negotiations within the scope of [the] agency.'" *Horwitz*, 816 N.E.2d at 279 (citing *Hoffman & Morton Co. v. American Insurance Co.*, 181 N.E.2d 821 (Ill. App. Ct. 1962)). Counter-Defendants do not contend that such circumstances are present here.

Lastly, Counter-Defendants argue that the merger clause in the MSAs precludes interpreting the MSAs in light of Counter-Defendants' contracts with other entities. [595, at 13.] Specifically, the MSAs provide:

> This Agreement contains the entire agreement of the parties with respect to their subject matter and supersedes all existing agreements and all other oral, written or other communications between them concerning their subject matter[.]

[595-1, at ¶ 18.A.] However, the merger clause addresses agreements between the parties to the contract, not agreements with third parties. Furthermore, it cannot be the case that Counter-Defendants' contracts with data integrators are irrelevant to determining whether the data integrators can be characterized as agents of Counter-Defendants. While Counter-Defendants' own characterization of their relationships with data integrators is not dispositive of the issue of agency, it certainly is relevant. *K.C. 1986 Ltd. P'ship v. Reade Mfg.*, 33 F.Supp.2d 820, 828 (W.D. Mo. 1998) ("While [the parties'] characterization of their relationship as an employer/independent contractor is not dispositive of the issue before the Court, it is probative of the intended nature of the relationship." (citations omitted)); *Bartolotta v. Dunkin' Brands Grp., Inc.*, 2016 WL 7104290,

---

between "an employee or agent and an independent contractor is the degree of retention by the employer or principal of the right to control the manner in which the details of the work are to be performed." *Jahns v. Milwaukee Mut. Ins. Co.*, 155 N.W.2d 674, 676 (Wis. 1968) (citations omitted). An independent contractor may be considered an agent for certain purposes—where the "fiduciary relationship has formed and the principal has control over certain activities." *Romero v. W. Bend Mut. Ins. Co.*, 885 N.W.2d 591, 601 (Wis. Ct. App. 2016) (citation omitted). Counter-Defendants have not identified any allegations indicating that such circumstances are present here.

at *5 (N.D. Ill. Dec. 6, 2016) ("In short, while the nature and extent of control as defined in the franchise agreement is relevant, so too is the parties' actual conduct and practice." (citations omitted)); *Ziehlsdorf v. Am. Family Ins. Grp.*, 461 N.W.2d 448 (Wis. Ct. App. 1990) ("A written agreement defining the relationship as an independent contractor is also a significant factor."). Indeed, even if the contracts between Counter-Defendants and data integrators did not characterize their relationship, looking at the terms of the contract likely would be relevant to engaging in the fact intensive agency analysis discussed above.

Based on the foregoing analysis, the Court denies Counter-Defendants' motion to dismiss CDK's breach of contract counterclaim.

B. Computer Fraud and Abuse Act (Second Counterclaim)

Counter-Defendants move for dismissal of CDK's counterclaim under the Computer Fraud and Abuse Act ("CFAA") because the counterclaim (1) is untimely, (2) fails to allege "accessor" liability against Counter-Defendants, and (3) CDK has not alleged the requisite loss or damage. The Court addresses each of these arguments in turn.

i. Time-Barred

Counter-Defendants move for dismissal of CDK's CFAA counterclaim as time-barred. Dismissal based on a statute of limitations is an affirmative defense. See Fed. R. Civ. P. 8(c)(1). Nevertheless, "dismissal is appropriate when the plaintiff pleads [herself] out of court by alleging facts sufficient to establish the complaint's tardiness." *Cancer Found., Inc. v. Cerberus Capital Mgmt., LP*, 559 F.3d 671, 674-75 (7th Cir. 2009); see also *United States v. Lewis*, 411 F.3d 838, 842 (7th Cir. 2005) (explaining that dismissal is appropriate "where, as here, the allegations of the complaint itself set forth everything necessary to satisfy the affirmative defense, such as when a complaint plainly reveals that an action is untimely under the governing statute of limitations").

The CFAA has a two-year statute of limitations. See 18 U.S.C. § 1030(g) ("No action may be brought under this subsection unless such action is begun within 2 years of the date of the act complained of or the date of the discovery of the damage."); *Meyer Tech. Solutions, LLC v. Kaegem Corp.*, 2017 WL 4512918, at *1 (N.D. Ill. Oct. 10, 2017) (concluding that CFAA claims were barred when counter-plaintiff "discovered the damage flowing from the unauthorized access" more than two years before it filed its counterclaims).

CDK filed its counterclaims on February 22, 2019. [See 522.] CDK alleges facts establishing that it became aware of Counter-Defendants' alleged unauthorized access of CDK's DMS no later than June 2015. [522, at ¶ 92 (alleging that Counter-Defendants "became aware that CDK objected to unauthorized access to the CDK DMS by third parties like Authenticom no later than when CDK announced SecurityFirst in June 2015 and in all likelihood, much earlier").] Counter-Defendants identify additional allegations indicating that CDK learned of the alleged misconduct more than two years before it filed its counterclaims. [395, at 14.]

CDK argues that its CFAA counterclaim is not time-barred because it is a compulsory counterclaim. While the Seventh Circuit has held that "[a] counterclaim for affirmative relief may not be asserted if barred by the statute of limitations," *Chauffeurs, Teamsters, Warehousemen & Helpers, Local Union No. 135 v. Jefferson Trucking Co.*, 628 F.2d 1023, 1027 (7th Cir. 1980), the Seventh Circuit also has recognized in dicta that "[t]here is authority that the filing of a claim tolls the statute of limitations on any compulsory counterclaim, by analogy to the 'relation back' language of Rule 15." *Asset Allocation & Mgmt. Co. v. W. Employers Ins. Co.*, 892 F.2d 566, 571 (7th Cir. 1989) (citing *Burlington Industries, Inc. v. Milliken & Co.*, 690 F.2d 380, 389 (4th Cir.1982); 6 Wright & Miller, FEDERAL PRACTICE AND PROCEDURE § 1419 (1971)). Although the Seventh Circuit has not conclusively addressed that issue, courts in this District have held that the

filing of a claim tolls the statute of limitations on any compulsory counterclaim. *Seitz v. Beeter*, 2013 WL 409428, at *2 (N.D. Ill. Jan. 31, 2013) (collecting cases).

"Rule 13(a) defines a compulsory counterclaim as one that 'arises out of the transaction or occurrence that is the subject matter of the opposing party's claim.'" *Bd. Of Regents of Univ. Of Wisconsin Sys. v. Phoenix Int'l Software, Inc.*, 653 F.3d 448, 470 (7th Cir. 2011) (quoting Fed. R. Civ. P. 13(a)). The Seventh Circuit uses "a 'logical relationship' test to decide whether two matters are the same for purposes of Rule 13(a)." *Id*. Under this "flexible" approach, the Court must "consider the totality of the claims, including the nature of the claims, the legal basis for recovery, the law involved, and the respective factual backgrounds." *Id*. (quoting *Burlington Northern R.R. Co. v. Strong*, 907 F.2d 707, 711 (1990)) (internal quotation marks omitted). "Even if two claims are 'technically related,' the relationship between the claims may be insufficient to satisfy Rule 13(a) if the two claims are based on different theories and would raise different legal and factual issues." *Simon v. Nw. Univ.*, 2017 WL 25173, at *3 (N.D. Ill. Jan. 3, 2017) (citing *Burlington N. R. Co. v. Strong*, 907 F.2d 707, 711 (7th Cir. 1990)).

CDK argues that its CFAA counterclaim is compulsory because it overlaps with several of CDK's affirmative defenses. Specifically, one of CDK's defenses to the Counter-Defendants' antitrust claims is that CDK legally is entitled to control access to its DMS. Another of CDK's defenses is that precluding hostile access is procompetitive because it furthers legitimate security concerns. However, neither defense establishes that CDK's CFAA counterclaim is based on the same theory and implicates the same legal and factual issues as Counter-Defendants' antitrust claims. With respect to the first defense, whether CDK is entitled to control access to its DMS may relate to CDK's CFAA counterclaim, but it is not central to Counter-Defendants' antitrust claims. As prior decisions in this case have noted, even assuming that CDK was entitled to deny

certain parties' access to its DMS generally, CDK is "not free to withhold such approval pursuant to illegal arrangements." *In re Dealer Mgmt. Sys. Antitrust Litig.*, 313 F. Supp. 3d 931, 948 (N.D. Ill. 2018). With respect to the second defense, whether precluding hostile access is procompetitive because it furthers legitimate security concerns certainly relates to Counter-Defendants' antitrust claims, but it is not central to CDK's CFAA counterclaim. The Court recognizes that CDK's CFAA counterclaim and Counter-Defendants' antitrust claims have a common-origin—disputes relating to CDK's DMS. However, the CFAA counterclaim and the antitrust claims are based on different legal theories and will present different legal and factual issues.

In support of its argument that its CFAA counterclaim is compulsory, CDK cites *Moore v. New York Cotton Exchange*, 270 U.S. 593, 602 (1926). In that case, the plaintiff sued the New York Cotton Exchange under the antitrust laws, alleging that the Exchange had a monopoly on price quotations for cotton futures and was illegally precluding the plaintiff from accessing the quotations via telegraphic ticker service. The Exchange counterclaimed, asserting that the plaintiff, "though it had been refused permission to use the quotations of the New York exchange, was purloining them, or receiving them from some person who was purloining them, and giving them out to its members." *Id*. at 603. After the antirust claim was dismissed, the Supreme Court concluded that it had jurisdiction over the counterclaim because it arose out of the same transaction as the plaintiff's antitrust claim. *Id*. at 610. The Supreme Court stated:

> The refusal to furnish the quotations is one of the links in the chain which constitutes the transaction upon which appellant here bases its cause of action. It is an important part of the transaction constituting the subject-matter of the counterclaim. It is the one circumstance without which neither party would have found it necessary to seek relief. Essential facts alleged by appellant enter into and constitute in part the cause of action set forth in the counterclaim.

Id.

CDK argues that this case is on all fours with *Moore*. Specifically, CDK contends that—like the plaintiff in *Moore*—it refused to give third-party integrators like Authenticom access to its DMS and that Counter-Defendants—like the defendant in *Moore*—"purloined data" from CDK's DMS. The Court recognizes that there are similarities between this case and *Moore*. However, in *Moore*, the Supreme Court noted that "so close is the connection between the case sought to be stated in the bill and that set up in the counterclaim, that it only needs the failure of the former to establish a foundation for the latter." *Id*. As discussed above, the same cannot be said here. The Court therefore finds *Moore* to be distinguishable and concludes that CDK's CFAA counterclaim is not a compulsory counterclaim.

CDK further argues that even if its CFAA counterclaim is not compulsory, it nonetheless is timely to the extent that it is based on recent instances of unauthorized access. Counter-Defendants respond that the continuing violation exception does not apply to the CFAA. "The continuing violation doctrine allows a plaintiff to get relief for a time-barred act by linking it with an act that is within the limitations period." *Selan v. Kiley*, 969 F.2d 560, 564 (7th Cir. 1992). The purpose of the continuing violation doctrine "is to allow suit to be delayed until a series of wrongful acts blossoms into an injury on which suit can be brought." *Limestone Dev. Corp. v. Vill. of Lemont, Ill.*, 520 F.3d 797, 801 (7th Cir. 2008) (citations omitted). The doctrine applies when individual instances of alleged misconduct alone are not actionable, but the cumulative effect of a series of actions is enough to establish an actionable claim. *Id*.

"The 'continuing violation' exception to federal statutes of limitations only allows suit to be delayed in cases where the first instance of misconduct may be insufficient—and indeed the 'cumulative effect' of a series of acts is necessary—to make out an actionable claim." *Meyer Tech. Sols., LLC v. Kaegem Corp.*, 2017 WL 4512918, at *1 (N.D. Ill. Oct. 10, 2017) (citing *Limestone*

Dev. Corp. v. Village of Lemont, Ill., 520 F.3d 797, 801 (7th Cir. 2008)).[4] Here, CDK does not identify any facts indicating that its CFAA counterclaim is based on the cumulative effect of a series of acts. Plaintiff therefore has not alleged facts sufficient to invoke the continuing violation exception. *Id*. Still, to the extent that CDK seeks to bring a CFAA counterclaim based on recent instances of unauthorized access, the continuing violation doctrine is not necessary to save CDK's CFAA counterclaim.

In sum, to the extent that CDK's CFAA counterclaim is based on misconduct occurring more than two years before CDK filed its counterclaims, the counterclaim is time-barred and is dismissed. However, to the extent that CDK's CFAA counterclaim is based on more recent conduct (since February 22, 2017), the claim is timely.

ii. Accessor Liability

Counter-Defendants also move for dismissal of CDK's CFAA counterclaim on the ground that CDK fails sufficiently to allege "accessor" liability on the part of Counter-Defendants. The CFAA provides criminal and civil penalties for anyone who "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains * * * information from any protected computer." 18 U.S.C. § 1030(a)(2)(C). Counter-Defendants seek dismissal of the CFAA counterclaim because "the complained-of computer access was conducted by persons other

[4] In *Meyer*, the court correctly noted that "[t]he 'continuing violation' exception to federal statutes of limitations only allows suit to be delayed in cases where the first instance of misconduct may be insufficient—and indeed the 'cumulative effect' of a series of acts is necessary—to make out an actionable claim." 2017 WL 4512918, at *1 (N.D. Ill. Oct. 10, 2017) (citing *Limestone Dev. Corp. v. Village of Lemont, Ill.*, 520 F.3d 797, 801 (7th Cir. 2008)). CDK indicates that *Meyer* stands for the proposition that the continuing violation doctrine does not apply to claims brought under the CFAA. However, the court did not go so far. Rather, it concluded that the continuing violation doctrine did not apply in that case. *Id*. Still, to the extent that the court in *Meyer* dismissed CFAA claims that were based on conduct occurring within the statute of limitations period, this Court respectfully disagrees that such claims should be dismissed as time-barred because misconduct also occurred outside of the limitations period. See *Gajewski v. Ocwen Loan Servicing*, 650 F. App'x 283, 287 (7th Cir. 2016) (considering whether the plaintiff sufficiently stated a claim with respect to alleged misconduct occurring within the statute of limitations period after rejecting invocation of the continuing violation doctrine).

than the dealerships—namely, 'Authenticom and other third parties.'" [595, at 15.] In other words, Counter-Defendants contend that CDK's CFAA counterclaim fails because CDK does not allege that Counter-Defendants personally accessed CDK's DMS.

Counter-Defendants begin by arguing that Court should not impose liability for inducing misconduct unless the statute expressly establishes inducer liability, which the CFAA does not. As noted by Counter-Defendants, Congress has imposed inducer liability in other statutes. See, *e.g.*, 35 U.S.C. § 271(b) ("Whoever actively induces infringement of a patent shall be liable as an infringer."). Still, the Court must examine the text of the statute. *United States v. Miscellaneous Firearms, Explosives, Destructive Devices and Ammunitions*, 376 F.3d 709, 712 (7th Cir. 2004) ("The cardinal rule of statutory interpretation is that courts 'must first look to the language of the statute and assume that its plain meaning accurately expresses the legislative purpose.'" (quoting *Grzan v. Charter Hosp. of Northwest Ind.*, 104 F.3d 116, 122 (7th Cir. 1997)). The statute at issue here—the CFAA—prohibits intentionally accessing a computer without authorization or in excess of authorized access. The question before the Court therefore is what it means to intentionally access a computer.

In *Synthes, Inc. v. Emerge Med., Inc.*, the court noted that the "the plain language of the statute requires only 'access'—no modifying term suggesting the need for 'personal access' is included." 2012 WL 4205476, at *17 (E.D. Pa. Sept. 19, 2012). Because the term "access" generally means "gaining admission to," *id*. (collecting authorities on the common meaning of the term "access"), many courts addressing the issue have concluded that direct personal access is not required. *Id*. (collecting cases). Still, courts are divided on the issue. For example, in *Power Equipment Maintenance, Inc. v. AIRCO Power Services, Inc.*, the court dismissed a CFAA claim against a defendant who allegedly "accessed files by having an administrative assistant print a

confidential contract for him" after his access had been revoked because he did not personally access the computer. 953 F. Supp. 2d 1290, 1297 (S.D. Ga. 2013). The defendant just "managed to convince another with access to provide him with the information." *Id*. The Court questions whether the CFAA should be read so narrowly, as such a reading would allow parties easily to circumvent the CFAA by enlisting unknowing persons to access computers personally. However, the Court need not resolve that issue now, as conspiracy is an express basis for liability under the CFAA. 18 U.S.C. § 1030(b) ("Whoever conspires to commit or attempts to commit an offense under subsection (a) of this section shall be punished as provided in subsection (c) of this section."). Counter-Plaintiff recognizes that it "did not plead a conspiracy claim in its Counterclaims." [639, at 15 n.4.] Still, CDK asserts that it has alleged sufficient facts to state a conspiracy claim under the CFAA. [*Id*.] Counter-Defendants do not explain why the facts alleged are insufficient to state a claim under the CFAA. Instead, Counter-Defendants assert that a brief cannot amend a pleading. Although that is true, the parties are required to plead facts, not causes of action. *Alioto v. Town of Lisbon*, 651 F.3d 715, 721 (7th Cir. 2011) ("[W]e have stated repeatedly (and frequently) that a complaint need not plead legal theories[.]"). Thus, as long as CDK alleged sufficient facts to bring a conspiracy counterclaim under the CFAA, it may proceed under that theory. Because Counter-Defendants do not address whether CDK alleged sufficient facts to bring a conspiracy claim under the CFAA, the Court denies their motion to dismiss the CFAA counterclaim for failure to allege wrongful conduct by Counter-Defendants.[5]

[5] Counter-Defendants do argue that it would be futile to allow CDK to amend its Counterclaims, citing one decision questioning whether the CFAA permits a conspiracy claim. [674, at 19.] However, that case cited did not rule on that issue. Because Counter-Defendants do not otherwise develop the argument, the Court will not consider it at this time. See *Crespo v. Colvin*, 824 F.3d 667, 674 (7th Cir. 2016) ("'[P]erfunctory and undeveloped arguments, and arguments that are unsupported by pertinent authority, are waived (even where those arguments raise constitutional issues).'" (quoting *United States v. Berkowitz*, 927 F.2d 1376, 1384 (7th Cir. 1991))).

Counter-Defendants further argue that—even if allegations of personal access are not necessary to state a claim under the CFAA— CDK's CFAA counterclaim still should be dismissed because CDK alleges that Counter-Defendants authorized Authenticom and other data integrators to access the DMS. Specifically, Counter-Defendants argue that the "authorization" required under the CFAA is that of the computer system's user, not the owner. [595, at 17.] However, Counter-Defendants do not cite any authority in support of that interpretation.

In any event, the Court rejects Counter-Defendants' interpretation of the CFAA. Although the statute does not specify whose authorization is necessary, it cannot be the case that only the user's authorization is necessary. As noted above, anyone who "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains * * * information from any protected computer" violates the CFAA. 18 U.S.C. § 1030(a)(2)(C). "Under the CFAA, the phrase '"exceeds authorized access" means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accessor is not entitled to obtain or alter.'" *Motorola, Inc. v. Lemko Corp.*, 609 F. Supp. 2d 760, 767 (N.D. Ill. 2009) (quoting 18 U.S.C. § 1030(e)(6)). Thus, "[a]llegations that an employee e-mailed and downloaded confidential information for an improper purpose are sufficient to state a claim that the employee exceeded her authorization." *Id*. (citing *Mintel Int'l Group, Ltd. v. Neergheen*, 2008 WL 2782818, at *3 (N.D. Ill. July 16, 2008)). In such cases, the employee would be the user. It would be illogical to say that the employee needed authorization from herself. Because the CFAA contemplates that users may exceed authorized access, it cannot be the case that the authorization required by the CFAA is that of the user. This Court previously concluded the authorization required by the CFAA is that of the owner of the computer system, not from anyone who happens to use the system. [506,

at 15.] And Counter-Defendant's have not presented persuasive grounds for reconsidering that conclusion.[6]

Finally, Counter-Defendants argue that the CFAA counterclaim fails because CDK alleges that it actually did authorize Authenticom and other third-party data integrators to access its DMS by contractually permitting dealerships to provide DMS access to their "agents." [595, at 17.] However, as discussed above, whether Authenticom and other third-party data integrators are agents of Counter-Defendants is an issue of fact not properly resolved on Counter-Defendant's motion to dismiss. Furthermore, CDK alleges that Counter-Defendants exceeded any authorization by—among other conduct—"having new credentials created and/or by restoring disabled credentials—including on information and belief by automated means." [*Id*. at ¶ 152.] These allegations are sufficient to state a claim under the CFAA. See *Tracfone Wireless, Inc. v. Simply Wireless, Inc.*, 229 F. Supp. 3d 1284, 1297 (S.D. Fla. 2017) (concluding that "the unauthorized or in excess of authorization elements" of the CFAA were sufficiently plead where plaintiff alleged "the sale of the unbundled PINs was not authorized by the agreement between the parties"). Accordingly, the Court denies Counter-Defendants' motion to dismiss for failure to allege accessor liability.

[6] Counter-Defendants do note that the CFAA is a penal statute that imposes criminal liability and that any ambiguities in the language should be resolved in the dealership's favor under the rule of lenity. However, "[t]he rule does not apply when a statute is unambiguous or when invoked to engraft an illogical requirement to its text." *Salinas v. United States*, 522 U.S. 52, 66 (1997) (citing *United States v. Shabani*, 513 U.S. 10, 17 (1994)).

iii. Requisite Losses

Counter-Defendants also argue that CDK fails to allege "loss to 1 or more persons during any 1-year period * * * aggregating at least $5,000 in value," as required by 18 U.S.C. § 1030(c)(4)(A)(i)(I).[7] CDK alleges that:

> The Dealership Counter-Defendants' violations of the CFAA have caused CDK to suffer damages and losses. These damages and losses include the costs of investigating and responding to the Dealership Counter-Defendants' unlawful actions; the costs of restoring the DMS and the data it contains to their condition prior to the Dealership Counter-Defendants' unlawful actions; and all revenue lost, costs incurred, and other consequential damages incurred because of disruption of service caused by the unlawful actions of the Dealership Counter-Defendants and the third parties acting in concert with the Dealership Counter-Defendants. On information and belief, these losses have exceeded $5,000 within a twelve-month period.

[522 (Counterclaims), at ¶ 144.] Counter-Defendants argue that this allegation is insufficient to establish the requisite amount of losses because CDK cannot aggregate the losses allegedly caused by all Counter-Defendants. Counter-Defendants further note that—based on this allegation—"each of the dealerships could have caused as little as $294.12 in alleged losses." [595, at 18 n.7.]

CDK argues that, "even assuming that a plaintiff must identify $5,000 in loss or damage attributable to each defendant, the defendants' contention that this standard has not been met was "simply one inference of many that [may] be drawn from Plaintiff's complaint." [638, at 18 (quoting *Wolf v. Schadegg*, 2016 WL 1117364 (D. Colo. Mar. 21, 2016)).] In other words, CDK believes that the Court should not infer that each Defendant caused as little as $294.12 in losses because that is just one possible inference and the Court must draw all reasonable inferences in Counter-Plaintiff's favor at the motion to dismiss stage. That argument misses the mark. Although the Court must draw all reasonable inferences in CDK's favor, that does not relieve CDK of its

[7] Counter Defendants also argue that CDK fails sufficiently to allege damage. However, Section 1030(c)(4)(A)(i)(I) does not address damage.

obligation to allege sufficient facts to establish the elements of its counterclaims, including that it satisfied the CFAA losses threshold.

In *Wolf*, the court concluded that the plaintiff alleged losses sufficient to satisfy the CFAA losses threshold even though it did not identify what specific loss was caused by each defendant. 2016 WL 1117364, at *4. In reaching that conclusion, however, the court noted that plaintiff's allegations permitted "an inference that both [d]efendants were working together to access [p]laintiffs' data, particularly given that [d]efendants were working for the same rival company and undoubtedly were familiar with each other by virtue of their past employment with [p]laintiff." *Id*. Here, on the other hand, CDK does not identify any facts indicating that Counter-Defendants were acting together.

CDK further argues that "allocation questions are at best fact issues that cannot be resolved on a motion to dismiss." [639, at 19 (citations omitted).] Even if that is the case, however, CDK fails directly to address the threshold issue of whether losses caused by each Defendant can be aggregated under the CFAA in the first place.[8] The Seventh Circuit has not yet addressed whether losses allegedly caused by multiple defendants can be aggregated for the purposes of satisfying the CFAA's loss threshold, and there is little case law on the issue.

In the context of determining whether losses incurred by multiple victims can be aggregated, however, courts have reached different conclusions. In *In re DoubleClick Inc. Privacy Litigation*, the court held "that damages and losses under § 1030(e)(8)(A) may only be aggregated across victims and over time for a single act." 154 F. Supp. 2d 497, 523 (S.D.N.Y. 2001). In reaching that conclusion, the court noted that the CFAA provides that "the term 'damage' means any impairment to the integrity or availability of data, a program, a system, or information that—

[8] The issue of how claimed losses should be allocated is different from the issue of whether claimed losses caused by numerous defendants can be aggregated.

(A) causes loss aggregating at least $5,000 in value during any 1–year period to one or more individuals." Because Section 1030(e)(8)(A) "is phrased in the singular ('any impairment to the integrity or availability of data, a program, a system, or information that—(a) causes loss'), rather than the plural (*e.g.*, any impairments to the integrity or availability of data, programs, systems, or information that—(a) cause loss * * *)," the court concluded that Section 1030(e)(8)(A) "should only apply to single acts." *Id*. at 523. The court found support for this conclusion in the Senate Judiciary Committee's report that accompanied the CFAA, *id*., which states:

> The Committee does not intend that every victim of acts proscribed under [1030(e)(8)(A)] must individually suffer a loss of [then] $1,000. Certain types of malicious mischief may cause smaller amounts of damage to numerous individuals, and thereby collectively create a loss of more than $1,000. By using 'one of more others', the Committee intends to make clear that losses caused by the same act may be aggregated for the purposes of meeting the [then] $1,000 threshold.

[Sen. R. No. 99-432.] The court in *DoubleClick* therefore concluded that Section "1030(e)(8)(A) only allows aggregation of damage over victims and time for a single act." *In re DoubleClick Inc. Privacy Litig.*, 154 F. Supp. 2d at 524. The Court noted that "[t]his interpretation is consistent with Congress' overall intent to limit the CFAA to major crimes." *Id*. at 523-24.

The Ninth Circuit reached the opposite conclusion in *Creative Computing v. Getloaded.com LLC*, 386 F.3d 930, 934 (9th Cir. 2004). Specifically, the court held that "[t]he damage floor in the [CFAA] contains no 'single act' requirement." 386 F.3d 930, 935 (9th Cir. 2004). In reaching that conclusion, the court asserted that "[t]he syntax makes it clear that * * * the $5,000 floor applies to how much damage or loss there is to the victim over a one-year period, not from a particular intrusion." *Id*. at 934. The court further asserted that even though the term "impairment" is singular, "impairment" can refer to multiple intrusions. *Id*. at 934-35 ("Multiple intrusions can cause a single impairment, and multiple corruptions of data can be described as a single 'impairment' to the data.").

Here, the Court need not resolve whether aggregation only is appropriate when losses stem from a single act (*i.e.*, the *DoubleClick* approach), or, alternatively, from multiple acts that accurately can be characterized as an impairment (*i.e.*, the *Creative Computing* approach), as CDK fails to allege facts indicating that Counter-Defendants were acting together and that their alleged wrongs can therefore be treated as an impairment. Nothing in either *DoubleClick* or *Creative Computing* indicates that losses caused independent actions of unrelated parties can be aggregated for the purposes of satisfying the CFAA's loss threshold. Such an interpretation of the CFAA would be inconsistent with the text of the statute.

The Court sees no reason to interpret the singular term "impairment" to encompass multiple unrelated wrongs. And nothing in the language indicates that a single victim can aggregate losses caused by multiple acts of multiple defendants.[9] CDK fails sufficiently to explain why the losses resulting from the alleged misconduct of separate defendants should be considered an "impairment" under the CFAA. Accordingly, the Court grants Counter-Defendants' motion to dismiss CDK's CFAA counterclaim for failure to allege sufficient losses. This dismissal is without prejudice to the filing of amended counterclaims by the date set forth above.

[9] As noted by CDK, the court in *Wolf* stated that "there appear to be no cases determining whether a plaintiff is required to meet the $5,000 floor with respect to each defendant individually or all defendants collectively." 2016 WL 1117364, at *4. The court went on to conclude that "who caused the alleged loss sustained by [p]laintiffs and to what degree each individual caused this loss" are "questions of fact whose answers are not necessarily available to [p]laintiffs prior to discovery." *Id*. This Court respectfully disagrees with that position. Even if an issue presents a factual issue, that does not relieve plaintiffs of their obligation to allege sufficient facts to state a claim. Although CDK asserts that the holding of *Wolf* is consistent with *Motorola, Inc. v. Lemko Corp.*, 609 F. Supp. 2d 760 (N.D. Ill. 2009), the Court again disagrees. In *Motorola*, the court concluded that the allegation that all defendants "caused [plaintiff] to incur losses of over $5,000 during a one-year period related to damage and security assessments" was "sufficient to allege loss for purposes of the CFAA." *Id*. at 768. However, in *Motorola*, the Court did not specifically address whether plaintiff could aggregate losses allegedly caused by multiple defendants, and the issue was not raised in the motion to dismiss. [Case No. 08-cv-5427, Dkt. 21.]

C. Digital Millennium Copyright Act (Third Counterclaim)

CDK brings a counterclaim against Counter-Defendants Continental and Warrensburg, alleging that they violated Section 1201(a)(1)(A) of the Digital Millennium Copyright Act ("DMCA"). The DMCA provides, in relevant part, that "[n]o person shall circumvent a technological measure that effectively controls access to a work protected under this title." 17 U.S.C. § 1201(a)(1)(A). The DMCA defines "circumvent a technological measure" to mean "descramble a scrambled work, to decrypt an encrypted work, or otherwise to avoid, bypass, remove, deactivate, or impair a technological measure, without the authority of the copyright owner." *Id*. at § 1201(a)(3)(A). The DMCA further defines the term to "circumvent protection afforded by a technological measure" to mean "avoiding, bypassing, removing, deactivating, or otherwise impairing a technological measure." *Id*. at § 1201(b)(2)(A).

CDK alleges that Counter-Defendants Continental and Warrensburg "circumvent[ed] a technological measure" that controls access to CDK's DMS by "provid[ing] dealer login credentials to Authenticom and other third parties in violation of contractual requirements that such credentials be given to and used only by authorized dealer employees." [522 (Counterclaims), at ¶ 151.] CDK further alleges that these Counter-Defendants and Authenticom worked to evade CDK's efforts to disable the login credentials "by having new credentials created and/or by restoring disabled credentials—including on information and belief by automated means." [*Id*. at ¶ 152.] Finally, CDK alleges that Counter-Defendants Continental and Warrensburg "installed Authenticom's Profile Manager tool in an attempt to re-enable" passwords that CDK had disabled. [*Id*. at ¶ 113.]

Counter-Defendants Continental and Warrensburg argue that they cannot be held secondarily liable under Section 1201(a)(1)(A) of the DMCA. In support of that argument,

Counter-Defendants cite cases holding that there is no secondary liability under various other statutes in "the absence of the words 'aid' or 'abet' in the statute indicates a congressional intent to not provide for aiding and abetting liability." *Wooley v. Jackson Hewitt, Inc.*, 540 F. Supp. 2d 964, 976 (N.D. Ill. 2008). However, the absence of such language does not establish that imposing any kind of secondary liability under the DMCA is improper, especially in light of the relationship between the DMCA and the Copyright Act, which does impose such liability.[10] "Congress enacted the DMCA in 1998 to comply with international copyright treaties and to update domestic copyright law for the online world." *Ellison v. Robertson*, 357 F.3d 1072, 1076 (9th Cir. 2004) (citations omitted); see also *Navistar, Inc. v. New Baltimore Garage, Inc.*, 2012 WL 4338816, at *3 (N.D. Ill. Sept. 20, 2012) ("Congress enacted the DMCA * * * to strengthen copyright protection in the digital age." (citation and internal quotation marks omitted)). Secondary liability is "well established" in the copyright context. *Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd.*, 545 U.S. 913, 930 (2005). Despite the fact that the copyright statute does not include language expressly addressing secondary liability, "vicarious liability is imposed in virtually all areas of the law, and the concept of contributory infringement is merely a species of the broader problem of identifying the circumstances in which it is just to hold one individual accountable for

[10] In discussing secondary liability, Counter-Defendants address numerous types of secondary liability (*e.g.*, aiding and abetting liability). CDK's opposition brief makes clear that they are proceeding on vicarious and contributory liability theories. Specifically, CDK draws comparisons between the DMCA and the Copyright Act, noting that the latter allows for claims based on vicarious and contributory infringement. [See 639, at 26.] Counter-Defendants fail to explain why contributory liability would not apply. Although Counter-Defendants assert that vicarious liability does not apply in a footnote [674, at 19 n.9], they fail fully to develop the argument. Because Counter-Defendants fail fully to explain why Counter-Plaintiff may not proceed under vicarious and/or contributory liability theories, the Court addresses Counter-Defendants' central argument that there is no secondary liability under the relevant provision of the DMCA. Counter-Defendants are free to fully develop any arguments with respect to vicarious and/or contributory liability under the DMCA in any future motion before the Court. Because CDK sufficiently alleges primary liability under the DMCA, as discussed below, CDK's DMCA counterclaim would survive regardless of whether CDK sufficiently alleged vicarious and/or contributory liability.

the actions of another." *Sony Corp. of Am. v. Universal City Studios, Inc.*, 464 U.S. 417, 435 (1984).[11]

Courts therefore have applied secondary liability principles drawn from copyright law to claims brought under the DMCA. See, *e.g., Gordon v. Nextel Commc'ns*, 345 F.3d 922, 925 & n.1 (6th Cir. 2003); *Microsoft Corp. v. Silver Star Micro, Inc.*, 2008 WL 115006, at *8 n.8 (N.D. Ga. Jan. 9, 2008) (citing *Ellison*); *Rosenthal v. MPC Computers, LLC*, 493 F. Supp. 2d 182, 190 (D. Mass. 2007) (citing *Gordon*). Counter-Defendants do not argue that these cases incorrectly were decided. Rather, Counter-Defendants argue that these cases are distinguishable because they relate to different provisions of the DMCA.

Although these cases do relate to different provisions of the DMCA, the Court sees no reason that common law vicarious liability principles would apply to these provisions but not Section 1205(a)(1). Counter-Defendants argue that the Court should not extend secondary liability principals to Section 1201(a) because that provision created a distinct anti-circumvention right under Section 1210(a) without any infringement nexus requirement. Thus, according to Counter-Defendants, attaching a copyright context to this provision of the statute would be improper. The Court disagrees. As noted by the Supreme Court in *Sony*, the secondary liability principles applied in copyright law stemmed from more generally applicable common law principles. Counter-Defendants have not identified any basis for concluding that such principles do not also apply to Section 1201(a).[12]

[11] Although CDK cites *Sony* and *Goldwyn-Mayer*, the Supreme Court cases setting forth these principles, Counter-Defendants fail entirely to address these cases in their reply.

[12] Although CDK has not cited any case finding a defendant liable under Section 1201(a)(1)(A) without personally engaging in such misconduct, Counter-Defendants do not cite any case rejecting such a theory. Counter-Defendants do cite *GC2 Inc. v. Int'l Game Tech.*, which concluded that the DMCA "imposes liability for violations by a defendant, not a third party." 2018 WL 5921315, at *8 (N.D. Ill. Nov. 12, 2018). However, that decision did not address secondary liability. Furthermore, the cited portion of that decision

In any event, CDK alleges facts sufficient to establish that Counter-Defendants themselves circumvented a technological measure that effectively controls access to a work protected under this title. Although it is true—as Counter-Defendants contend—that the use of valid username/password combinations alone is insufficient to establish liability under Section 1201(a)(1)(A) of the DMCA, *Navistar, Inc*, 2012 WL 4338816, at *5 (quoting *Egilman v. Keller & Heckman, LLP*, 401 F. Supp. 2d 105, 112 (D.D.C. 2005)); see also *Ground Zero Museum Workshop v. Wilson*, 813 F. Supp. 2d 678, 692 (D. Md. 2011) (recognizing same), CDK alleges that Counter-Defendants Continental and Warrensburg did more than simply provide Authenticom with valid passwords. Specifically, CDK claims that these Counter-Defendants took affirmative steps—including the installation of computer programs and/or the use of other automated programs—to circumvent CDK's efforts to prevent Authenticom's alleged unauthorized access of its DMS. For example, CDK alleges that these Counter-Defendants worked to evade "blocking by having new credentials created and/or by restoring disabled credentials—including on information and belief by automated means." [522 (Counterclaims), at ¶ 152.] These allegations are sufficient to establish primary liability at the motion to dismiss stage. *In re Dealer Mgmt. Sys. Antitrust Litig.*, 362 F. Supp. 3d 558, 571 (N.D. Ill. 2019).

Counter-Defendants also argue that CDK conflates Section 1201(a)(1)(A) and Section 1201(a)(2). As noted above, Section 1201(a)(1)(A) provides, in relevant part, that "[n]o person shall circumvent a technological measure that effectively controls access to a work protected under this title." 17 U.S.C. § 1201(a)(1)(A). Section 1201(a)(2) states, in relevant part, that "[n]o person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that (A) is primarily designed or

addressed an issue that the court declined to address because the arguments were not sufficiently developed. *Id*.

produced for the purpose of circumventing a technological measure that effectively controls access to a work protected under this title." *Id*. at § 1201(a)(2). According to Counter-Defendants, Section 1201(a)(1)(A) "addresses the 'conduct' of actually circumventing a technological measure, whereas [Section] 1201(a)(2) addresses the underlying process of how the circumvention occurred." [674, at 23.] Counter-Defendants therefore contend that Section 1201(a)(1)(A) does not apply to them "as they did not engage in the actual act of the alleged circumvention." [*Id*.] However, Counter-Defendants misread the statute. Section 1201(a)(2) "prohibits *devices* primarily designed to circumvent effective technological measures that limit access to a work." S. REP. 105-190, at 12 (emphasis added). Even if CDK cited the incorrect provision of the statute, that would not mandate dismissal. *Suarez v. W.M. Barr & Co., Inc.*, 842 F.3d 513, 518 (7th Cir. 2016). Regardless, as discussed above, CDK does allege that Continental and Warrensburg engaged in conduct amounting to a circumvention of a technological measure.[13]

Finally, Counter-Defendants raise a number of additional arguments in support of the dismissal of CDK's DMCA counterclaim that were not raised in their initial motion to dismiss. Specifically, Counter-Defendants argue that CDK has not sufficiently alleged "access to a work protected" under 17 U.S.C. § 1201(a)(1)(A). Counter-Defendants also argue that their conduct is exempted under 17 U.S.C. § 1201(f)(2). Because Counter-Defendants first raised these arguments in their reply brief, the arguments are waived.[14] *West*, 81 F. App'x 74, 75. Accordingly, the Court

[13] Continental and Warrensburg focus on allegations that they improperly provided and/or used valid username and password combinations. Again, while those allegations do not amount to DMCA violations, they do not make otherwise prohibited conduct permissible. Furthermore, the fact that Authenticom used automated programs to re-enable login credentials does not foreclose the possibility that Continental and Warrensburg also engaged in the misconduct.

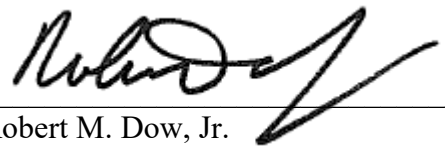
[14] The Court notes that CDK filed a sur-reply touching on these issues. [691.] In the sur-reply, CDK identifies reasons why these arguments fail. Although these arguments appear to be meritorious at first glance, Counter-Defendants have not had the opportunity to respond to the arguments. The Court therefore

denies Counter-Defendants Continental and Warrensburg motion to dismiss CDK's DMCA claims.

IV. Conclusion

For the reasons set forth above, the motion to dismiss the counterclaims of Defendant/Counter-Plaintiff CDK Global, LLC [593] is granted in part and denied in part. Counter-Plaintiff is given until September 30, 2019 to file amended counterclaims consistent with this opinion.

Date: September 3, 2019



Robert M. Dow, Jr.
United States District Judge

defers issuing a definitive ruling on these issues until they properly are presented to the Court at a future stage of the case.